

RMT:SK/AFM/MTK
F.#2018R00645

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - -X

UNITED STATES OF AMERICA

- against -

SERGEY OVSYANNIKOV,
EVGENY TIMCHENKO and
ALEXANDER ISAEV,

Defendants.

TO BE FILED UNDER SEAL

COMPLAINT AND
AFFIDAVIT IN
SUPPORT OF
APPLICATION FOR
ARREST WARRANTS

(18 U.S.C. § 1349)

Case No. 18-MJ-625

- - - - -X

EASTERN DISTRICT OF NEW YORK, SS:

EVELINA ASLANYAN, being duly sworn, deposes and states that she is a
Special Agent with the Federal Bureau of Investigation, duly appointed according to law and
acting as such.

In or about and between December 2015 and July 2018, both dates being
approximate and inclusive, within the Eastern District of New York and elsewhere, the
defendants SERGEY OVSYANNIKOV, EVGENY TIMCHENKO and ALEXANDER
ISAEV, together with others, did knowingly and intentionally conspire to devise a scheme
and artifice to defraud online advertising companies and businesses, and to obtain money and
property by means of materially false and fraudulent pretenses, representations and promises,
and for the purpose of executing such scheme and artifice, to transmit and cause to be
transmitted by means of wire communication in interstate and foreign commerce, writings,

signs, signals, pictures and sounds, to wit: electronic communications to computers and servers in the United States and elsewhere, emails and other online communications, and monetary transfers, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1349)

The source of your deponent's information and the grounds for her belief are as follows:¹

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since March 2012. I have been involved in the investigation of numerous cases involving cybercrime, financial fraud and money laundering, during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.
2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from:
(a) my personal participation in the investigation; (b) my review of the investigative file; and
(c) reports made to me by witnesses and other law enforcement officers involved in the investigation.

¹ Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

3. The FBI is conducting an investigation into online advertising fraud by certain individuals overseas. The government's investigation has uncovered evidence that the defendants SERGEY OVSYANNIKOV, EVGENY TIMCHENKO and ALEXANDER ISAEV executed an online advertising fraud scheme that victimized individuals and businesses in the United States and elsewhere. Specifically, the evidence obtained in the investigation shows that the defendants used computers that they controlled to create the illusion that a real human internet user was viewing an advertisement on a real internet webpage -- when, in fact, a computer was loading the advertisement on a counterfeit webpage via an automated program -- in order to fraudulently obtain a share of the resulting advertising revenue.

Background Regarding Online Advertising

4. Based on my knowledge, training and experience, and consultation with experts in online advertising, website owners (or "publishers") commonly use entities called supply-side platforms (or "SSPs") to find bidders for the advertising space on their websites. Businesses (or "brands") and their advertising companies commonly use entities called demand-side platforms (or "DSPs") to bid for advertising space on websites that real human internet users are browsing. These auctions are conducted by the SSPs, and take place in a span of milliseconds while a user is launching a webpage. This ecosystem functions to facilitate the brands' ability to advertise their goods and services online, and the publishers' ability to earn revenue for providing content online. The brands typically pay for advertising on a lump-sum basis, and website owners typically receive payment for the amount of internet traffic that is directed to the brands' advertisements, on a per-click or per-impression basis.

5. DSPs typically have direct relationships with advertising companies, but SSPs are not always in direct communication with publishers. Instead, the SSP and the publisher may be connected through a chain of intermediaries, known as advertising networks. This chain, which may be several entities deep, stretches toward the brand in one direction (the “demand side”) and toward the publisher in the other direction (the “supply side”). An advertising network’s partner typically supplies the advertising network with a snippet of code, known as an “ad tag,” that it wishes to have placed on publishers’ websites. The advertising network then agrees to ensure that the ad tag is placed in particular advertising slots on publisher’s webpages, either by negotiating with publishers directly or by contracting with other intermediaries.

6. Each time a user browses to a webpage that contains an ad tag, the user’s computer activates the ad tag. A signal (the “ad call”) is then sent to one or more SSPs putting the designated ad slot out for immediate bid by potential advertisers. The signal includes the IP address of the computer loading the tag, the URL of the page on which the tag was encountered, and some information regarding the intermediaries responsible for placing the tag.

7. When the bidder wins an advertising opportunity and the advertisement is served to the relevant advertising slot, a process is triggered that ultimately results in a payment moving from the demand side of the chain to the various intermediaries responsible for placing the ad tag on the webpage.

Online Advertising Fraud

8. Based on my knowledge, training and experience, and consultation with experts in cybercrime and online advertising fraud, “advertising fraud” is generally a

type of cybercrime in which malicious actors fraudulently obtain money from online advertising companies and businesses. In the subtype of advertising fraud known as an “impression” fraud scheme, internet advertisers are made to believe that advertisements they purchase are viewed by real human internet users (an occurrence known as an “impression”), when in fact the advertisements are automatically loaded onto computers controlled by the malicious actors and are not viewed by real human internet users.

9. In conjunction with the fake impressions, malicious actors carrying out an impression fraud commonly send out falsified data to fraudulently represent to SSPs that advertisements are being viewed by real human internet users, ultimately resulting in the issuance of payments by advertisers. The malicious actors have business arrangements in place that allow them to claim a portion of those payments. The process of falsifying data to indicate that an advertisement is being viewed by a real human internet user in the context of a particular website is known as “domain spoofing,” or, more simply, “spoofing.”

The Defendants’ Scheme

10. Based on the facts of this investigation, and as further described below, the defendants carried out their scheme by operating a purported advertising network called Adzos. Adzos had business arrangements with other advertising networks that enabled it to receive payment in return for placing ad tags with publishers on behalf of those advertising networks. Rather than place these ad tags on real publishers’ websites, however, Adzos made use of a network of compromised computers belonging to individuals and businesses in the United States and elsewhere, including in the Eastern District of New York. The computers were infected by malware, leading them to surreptitiously initiate connections with two computer servers controlled by the defendants. At the instruction of those servers,

the compromised computers purported to load webpages belonging to well-known publishers, including publishers in the Eastern District of New York. The compromised computers then sent signals to SSPs indicating that real human internet users were loading the webpages, and soliciting bids on the opportunity to show advertisements to those purported users. In response, DSPs bid on those opportunities. The winning DSPs made payments to SSPs (using money provided by brands) in return for the purported impressions, and the SSPs transferred those payments to advertising networks to be passed along the chain of intermediaries described above. Adzos stood at the end of this chain, claiming payment for the purported impressions.

11. Between approximately February 27, 2018 and June 13, 2018, the two computer servers controlled by the defendants made approximately 5.5 billion connections with approximately 1.7 million IP addresses, corresponding to compromised computers located around the world. Brands and advertising agency clients of SSPs incurred millions of dollars in losses by paying for fraudulent advertisements.

The Defendants Victimize a Business in the Eastern District of New York

12. As an example of the scheme described above, on or about May 17, 2018, an FBI agent and an FBI computer scientist visited the office of a business located in Blue Point, New York ("Victim-1").

13. With the consent of Victim-1's owner, the FBI personnel examined a computer at Victim-1's office that was connected to the internet and recorded the incoming and outgoing data for that computer for approximately 40 minutes. During the recording period, the FBI personnel did not enter any commands into the computer or direct the computer to make any specific internet connections. However, the recorded data revealed

that the computer had surreptitiously initiated connections with two computer servers associated with the IP addresses 66.85.77.82 and 66.85.77.83, respectively (the "Redirect Servers"), hosted at a server provider based in Kansas City, Missouri (the "Missouri Provider"). An examination of Victim-1's computer revealed that Victim-1's computer had been infected by malicious software which, among other things, directed Victim-1's computer to initiate connections with the Redirect Servers.

14. The recorded data revealed that the Redirect Servers caused Victim-1's computer to initiate connections with other servers and ultimately to send fraudulent communications to advertising companies. For example, one of the Redirect Servers sent a communication to Victim-1's computer containing the internet domain of an article hosted on a news and commentary website based in Los Angeles, California ("Publisher-1"). Victim-1's computer then visited a server associated with the IP address 5.45.79.34 (the "Fraudulent Content Server") and downloaded from the Fraudulent Content Server a counterfeit webpage that had in its title the name of the article and Publisher-1's name. The counterfeit webpage contained an internal placeholder (or "frame") with space for an advertisement to run, followed by approximately ten links to others articles published by Publisher-1. Victim-1's computer then connected once again to the Redirect Servers, triggering a process that resulted in Victim-1's computer receiving an ad tag from the Redirect Servers. The ad tag directed Victim-1's computer to contact an SSP located in New York, NY and offer up the advertising space on the counterfeit webpage for bidding. Victim-1's computer contacted the SSP more than three hundred times over the course of approximately eight minutes. In each instance, Victim-1's computer sent the SSP information including Victim-1's IP address, the URL of Publisher-1, the dimensions of the

frame in which the advertisement would play, and the technical specifications of the advertisement player.

15. In response, Victim-1's computer received an advertisement for Advertiser-1, a nonprofit hospital located in West Islip, New York. The advertisement ("Ad-1") was not seen by anyone at Victim-1 because it ran in a browser that the malicious actors had custom-designed to run invisibly in the background on Victim-1's computer.

Identification of the Malicious Actors

16. A review of records obtained from the Missouri Provider revealed that the Redirect Servers were also in communication with six servers hosted at a server provider based in Miami, Florida (the "Florida Provider"). These communications numbered, on average, approximately 1,000 to 2,000 communications per hour. Records obtained from the Florida Provider revealed that these six servers were registered to SERGEY OVSYANNIKOV with an email address identified herein as the "Target Email Account." Records obtained from the Florida Provider revealed that OVSYANNIKOV had rented six other servers from the Florida Provider, for a total of twelve servers (the "Backend Servers").² Records obtained from the Florida Provider also revealed that OVSYANNIKOV had logged into the Backend Servers from the IP address 178.62.111.215. A search of publicly available databases revealed that the foregoing IP address was associated with a server hosted at a server provider based in New York, New York (the "New York Provider"). Records obtained from the New York Provider revealed that the

² Based on my knowledge, training and experience, the facts of this investigation, and consultation with a computer scientist, and as further explained below, the Backend Servers served as command-and-control servers to further the fraud.

server associated with IP address 178.62.111.215 was registered to SERGEY OVSYANNIKOV with an email address of the Target Email Account. Records obtained from the New York Provider also revealed that OVSYANNIKOV had logged into his server at the New York Provider from the IP address 212.71.245.44. A search of publicly available databases revealed that the IP address 212.71.245.44 was associated with a server hosted at a server provider based in Galloway, New Jersey (the “New Jersey Provider”). Records obtained from the New Jersey Provider revealed that the server associated with the IP address 212.71.245.44 was registered to SERGEY OVSYANNIKOV.

17. On January 24, 2018, the Honorable Viktor V. Pohorelsky, United States Magistrate Judge for the Eastern District of New York, issued a search warrant for the Target Email Account. During the execution of the search warrant, law enforcement agents observed email communications and other records that appear to confirm that the Target Email Account was, indeed, used by SERGEY OVSYANNIKOV. For example, the user of the Target Email Account, among other things, received invoices addressed to SERGEY OVSYANNIKOV and sent contracts extended by SERGEY OVSYANNIKOV.

18. Law enforcement agents also observed in the search warrant returns for the Target Email Account a collaborative spreadsheet related to online advertising fraud and bearing the title “Adzos Structure. Hosting and Domains” (the “Adzos Infrastructure Spreadsheet”).³ The Adzos Infrastructure Spreadsheet contained a detailed list of computer servers used to victimize Victim-1, Publisher-1, and Advertiser-1. Specifically, the Adzos

³ Excerpts and summaries of online communications and documents may be drawn from draft and summary translations from Russian to English that are subject to revision.

Infrastructure Spreadsheet listed one of the Redirect Servers, with the notation “Proxy for Clicks Under RON”; the Fraudulent Content Server, with the notation “Sites Under RON (spoof)”; and all twelve Backend Servers. Based on my knowledge, training and experience, and consultation with experts in cybercrime and online advertising fraud, “RON” is an abbreviation for “Run of Network,” which is a method by which advertising companies place their clients’ advertisements on a broad range of webpages.

19. Law enforcement agents observed the metadata associated with the Adzos Infrastructure Spreadsheet, which revealed that two other individuals -- EVGENY TIMCHENKO and ALEXANDER ISAEV -- had privileges to access the spreadsheet. Specifically, TIMCHENKO had editing privileges and ISAEV had reading privileges.⁴

20. In addition to their email communications, OVSYANNIKOV, TIMCHENKO and ISAEV communicated using a specific online communications platform (the “Platform”). Based on my knowledge, training and experience, and a review of information provided by the Platform on its publicly accessible website, the Platform is an online project management tool that enables individuals to collaborate and communicate about ongoing projects. Users of the Platform can communicate on private internal

⁴ Records obtained from the Target Email Account revealed that both TIMCHENKO and ISAEV had separate email accounts that communicated with the Target Email Account. Records obtained from the service provider for TIMCHENKO’s and ISAEV’s accounts revealed that they were registered to “Yevgeniy Timchenko” and “Alex Adzos,” respectively, and were registered to separate telephone numbers. Records obtained from the Target Email Account revealed that ISAEV sent a copy of a passport containing his name and photograph to OVSYANNIKOV. A review of publicly available information revealed a social media profile purporting to be TIMCHENKO’s, and records obtained from the social media company revealed that the profile account was registered to TIMCHENKO’s email account.

discussion boards, designate certain project-related tasks on individual “cards,” and post comments and files to such cards.

21. Records obtained from the Target Email Account revealed that on December 24, 2015, OVSYANNIKOV created a user account on the Platform using the Target Email Account as his registration email (“Target Platform Account 1”). That same day, TIMCHENKO created a user account on the Platform on OVSYANNIKOV’s recommendation (“Target Platform Account 2”); the next day, ISAEV also created a user account on the Platform.

22. On January 24, 2018, the Honorable Viktor V. Pohorelsky, United States Magistrate Judge for the Eastern District of New York, issued a search warrant for Target Platform Account 1 and Target Platform Account 2 (the “Target Platform Accounts”). During the execution of the search warrant, law enforcement agents observed that OVSYANNIKOV, TIMCHENKO and ISAEV had created a collaborative project on the Platform related to online advertising fraud and used the Platform to communicate about the design and execution of the fraud.

23. For example, on or about April 20, 2016, OVSYANNIKOV posted a message on the Platform demonstrating a method for creating a fraudulent impression of a visit to the webpage of a major U.S. online retail company. OVSYANNIKOV explained to his co-conspirators: “you give me a company,” and then set forth a string of HTML code that included the text “spoof_domain=[retailer].com”; “the bot takes that link [and] sets itself accordingly”; the “spoofed domain” would be “[retailer].com” and the “host ip” would be “www2.” Based on my knowledge, training and experience, and the facts of this investigation, the “spoof_domain” is a reference to the real internet webpage that the

malicious actors counterfeit as part of their scheme, and the “bot” is a reference to a computer or computers within the malicious actors’ control. In addition, the Adzos Infrastructure Spreadsheet listed “www2” as the nickname for the Fraudulent Content Server, with a notation related to spoofing.

24. The conspirators also used the Platform to discuss operational issues related to the spoofing of the listed domains. For example, on or about May 10, 2016, OVSYANNIKOV posted a message stating, “For some reason traffic going to the spoof-domains is pulling the wrong VAST tag.” Based on my knowledge, training and experience, and consultation with experts in cybercrime and online advertising fraud, “VAST” is a reference to a standardized protocol for serving video advertisements.

25. On or about June 28, 2016, TIMCHENKO posted a message on the Platform identifying the Florida Provider as his preferred server provider to host the servers associated with the fraud, because it had the “coolest processors” and a “larger” cache than a competing provider.

26. By July 21, 2016, the conspirators created a card on the Platform with the title “New companies for spoofing.” The conspirators used this card to post and comment on lists of domains that they would spoof. For example, on or about September 21, 2016, TIMCHENKO commented that he had “added 336 more domains.” On the same day, TIMCHENKO commented that the domains included prominent online publishers, including the domains of multiple major U.S. technology companies. Over time, TIMCHENKO added many other publishers’ domains to the lists on the “New companies for spoofing” card, including the domains of several major U.S. news magazines.

27. From time to time, ISAEV also participated in and commented on the conversations occurring on the Platform. For example, on or about April 21, 2016, ISAEV posted a message to a card entitled “New server for www2.” The message read: “Hello. Centos 6 x64 installed. 5.45.79.34\nroot / 1JyxEg2jshpAyNO3.” “www2” is the nickname assigned to the Fraudulent Content Server in the Adzos Infrastructure Spreadsheet. Based on my knowledge, training and experience, and consultation with computer scientists, “CentOS” is a computer operating system, and “x64” refers to a computer with a 64-bit central processing unit.

28. On January 26, 2018, the Honorable Viktor V. Pohorelsky, United States Magistrate Judge for the Eastern District of New York, issued a search warrant for the Backend Servers. During the execution of the search warrant, law enforcement agents observed that the Backend Servers contained records and information that operated to further the fraud.

29. For example, each of the Backend Servers contained a configuration file listing servers associated with the fraud and listed in the Adzos Infrastructure Spreadsheet, including the Redirect Servers, the Fraudulent Content Server, and three other servers, collectively identified as “spoof_hosts.”

30. In addition, at least five of the Backend Servers contained lists of online publishers’ domains, which together included more than 3,000 individual domains. Each Backend Server contained computer code designed to respond to incoming communications from the Redirect Servers with a domain to be spoofed, an ad tag, and instructions to contact an advertising company.

31. Law enforcement agents also observed that the Backend Servers contained computer code consistent with the operation of the fraud as discussed by the conspirators on the Platform. For example, on or about June 25, 2016, TIMCHENKO noted a convention in the code that “Links href= are spoofed, Links src= are left as is.” The Backend Servers contained computer code designating domains to be spoofed with the prefix “href,” and domains to be contacted with the prefix “src=.”

32. Records obtained from the Target Email Account further revealed spreadsheets containing metrics related to advertising performance such as “eCPM” (a measure of estimated return per thousand advertising impressions) and the daily revenue associated with that performance. The spreadsheets and other documents in the Target Email Account reflected tens of thousands of dollars in revenue each week and distribution of that revenue to OVSYANNIKOV, TIMCHENKO and ISAEV, among others.

33. Law enforcement agents observed communications in the Target Email Account reflecting that Adzos⁵ had earned its revenue by purporting to place advertisements on websites where human users could see them. For example, agents observed an email from ISAEV to OVSYANNIKOV, dated April 15, 2017, attaching an agreement dated May 15, 2015 between Octmedia and another advertising network (“Ad Network-1”). In the agreement, ISAEV agreed to place online advertisements on behalf of Ad Network-1.

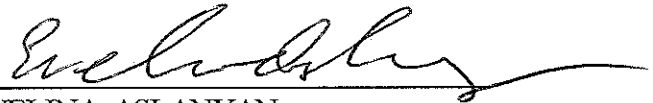
34. Law enforcement agents have reviewed records for a bank account in the Czech Republic whose registered accountholder is Octmedia. The records reveal that between in or around December 2016 and in or around May 2017, Ad Network-1 wired

⁵ Emails reviewed by law enforcement agents indicate that Adzos operated under the corporate name Octmedia LP.

approximately \$1.5 million into Octmedia's account. Notations contained in the banking records reflect that these transfers were payments for advertising traffic. The funds were subsequently wired from Octmedia's account to other entities, including an entity controlled by OVSYANNIKOV and another entity that in turn wired the funds to ISAEV.

35. Communications among the conspirators reflect that the services which Octmedia provided to Ad Network-1 were fraudulent. For example, on August 18, 2016, an employee of Ad Network-1 emailed OVSYANNIKOV a list of approximately 30 online publishers' domains requesting that OVSYANNIKOV "add [these] please[.]" The next day, TIMCHENKO added a list of domains to the "New companies for spoofing" card on the Platform that included all but two of the domains that the employee of Ad Network-1 had sent to OVSYANNIKOV the previous day. Furthermore, on August 1, 2017, records from the Platform reveal that OVSYANNIKOV posted a message to the "New companies for spoofing" card that discussed sending traffic to Ad Network-1.

WHEREFORE, your deponent respectfully requests that arrest warrants be issued for the defendants SERGEY OVSYANNIKOV, EVGENY TIMCHENKO and ALEXANDER ISAEV, so that they be dealt with according to law.



EVELINA ASLANYAN
Special Agent, Federal Bureau of Investigation

Sworn to before me this
31st

SIGO

THOMAS J. GOODYEN D. GO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK